

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

IN THE MATTER OF THE ARREST OF
JARED WILKES POST

Case No. 4:22-mj-00037-SAO

**AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Baron H. Lambert, being duly sworn, depose and say:

BACKGROUND

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") and have been so employed since March 6, 2005. Since October 2011, I have been assigned to the Anchorage Field Office, Fairbanks Resident Agency. I investigate violations of federal law in the State of Alaska, as well as other violations of law. I previously served as an Officer in the United States Army. I have training and experience in the enforcement of the laws of the United States, including the preparation and presentation of search warrant affidavits and in conducting searches pursuant to judicially authorized search warrants. I am an investigative law enforcement officer of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18 of the United States Code. I graduated from the FBI Academy in Quantico, Virginia and have received basic, advanced, and on-the-job training in the investigation of criminal violations of federal law.

2. This affidavit is in support of a criminal complaint and arrest warrant for JARED WILKES POST (POST), DOB 12/08/1996 for violations of 18 U.S.C. § 1344(2)

(bank fraud), violations of 18 U.S.C. § 1349 (conspiracy to commit bank fraud), and violations of 18 U.S.C. § 1028A (aggravated identity theft). The information herein is based upon my personal knowledge, interviews with witnesses, discussions I have had with other law enforcement officer, reports I have read, or from those specific sources as set forth.

STATEMENT OF PROBABLE CAUSE

3. In August 2018, the Fairbanks Police Department (FPD) referred a case to the FBI after receiving multiple complaints of bank fraud involving POST as far back as August 2017. Beginning on a date unknown but no later than 2017, and continuing until in or around January 2021, within the District of Alaska and elsewhere, POST and a co-conspirator L.S., together with others known and unknown, combined, conspired, and agreed with each other to knowingly and with intent to defraud, devise, execute, and attempt to execute a scheme to obtain monies, funds, assets, and other property owned by and in the custody and control of Alaska USA Federal Credit Union, Mt. McKinley Bank, U.S. Bank, Santander Bank, N.A., Key Bank, MAC Federal Credit Union, Citibank and Wells Fargo, by means of materially false and fraudulent pretenses, representations, and promises, and the concealment of material facts, in violation of 18 U.S.C. § 1344(2).

4. The scheme operated as follows: POST would contact individuals through social media such as Facebook or Instagram and convince them to provide their banking information in order to make quick money. Once the individual—referred to as “Plays”—provided their information, POST or L.S. would conduct a remote deposit of a check into their bank account. The “Plays” would then be asked to withdraw a portion of the deposit

to be provided to POST or L.S., while the “Play” would be told they could keep the remainder as payment for use of their account. In reality, POST knew that the remotely deposited checks were stolen, forged, or fraudulent checks that had been stolen from other actual persons in Alaska and elsewhere. POST would deposit and withdraw the funds in quick succession so that the cash withdrawal was completed before the bank caught the bad checks. This ultimately caused the “Plays” and their banks to suffer a loss if the fraudulent check deposits were subsequently reversed by the bank from which the fraudulent checks were drawn upon. If the deposits were not reversed, the victim whose checks were stolen and their banks suffered a loss. POST and L.S. obtained significant financial benefits from the scheme. In a variation described below, POST asks a “Play” to wire funds back to him through Western Union or similar such as Venmo, rather than making a cash withdrawal.

5. The scheme creates multiple victims. The first is the willing participant, or a “Play.” Some “Plays” believed POST was depositing legitimate checks. Others were convinced by POST that they could make quick money and participated in the scheme. The second victim is the true owner of the stolen or fraudulent check(s). The third victims are the banks of the “Plays.”

6. In furtherance of the conspiracy and to affect its illegal object, POST and L.S. and their co-conspirators committed the following overt acts, among others:

7. On or about August 14, 2017, POST deposited or caused to be deposited a fraudulent \$2,889 check drawn from a Citi Bank account, into an Alaska USA account in “Play” R.H.’s name.

8. On or about May 6, 2019, POST deposited or caused to be deposited a fraudulent \$650 check drawn from G.P.'s Wells Fargo bank account ending in -2651 in victim G.P.'s name, into U.S. Bank account ending in -6702 in "Play" S.G.'s name. POST utilized, without lawful authority, the name and bank account number of victim G.P. to commit this offense, knowing that G.P. was an actual person.

9. On or about May 6, 2019, POST deposited or caused to be deposited a fraudulent \$802 check drawn from G.P.'s Wells Fargo bank account ending in -2651 in victim G.P.'s name, into U.S. Bank account ending in -6702 in "Play" S.G.'s name. POST utilized, without lawful authority, the name and bank account number of victim G.P. to commit this offense, knowing J.H. was an actual person.

10. On or about October 30, 2019, L.S. and POST exchanged messages over Instagram regarding the scheme, with L.S. telling POST to send him \$1,000 for "Fraud shit" and later writing "You wanna be scammed?? Find out on the next episode of I got your log in."

11. On December 24, 2019, POST and L.S. continued to exchange messages about the scheme, with L.S. stating "social media be popping I post one thing and get 6-7 [bank] accounts in a day lol." L.S. continues that he's been "running my account off the same checks since last time we talked and I've made over 13k," referring to proceeds obtained from stolen or fraudulent checks.

12. On or about December 25, 2019, POST and L.S. continued to discuss the fraudulent scheme and POST requested that L.S. deposit two fraudulent checks into his "Plays" bank accounts. L.S. agreed and wrote "I'll do your accounts but I know your

running off but it's cool I literally been eating off the same checks the man has been out of town and I guess hasn't canceled them Imfaoo. They keep getting approved the denalis." POST replied "I'm not running off bro I just want my cut. And you do owe me." POST then sent L.S. the names and Alaska USA bank account login information for "Plays," D.P. and J.B., whom he describes as "Kids on my facebook." POST instructed L.S. "just do a regular mobile deposit," and L.S. replies "I already deposited into hers man [it] pops on the 26th smh." POST continued that he has the debit card for D.P.'s account. L.S. asks "how" POST obtained D.P.'s debit card, to which POST replied "he's a native kid from the village. He mailed it to me."

13. On or about December 26, 2019, L.S. messaged POST "Ima do the accounts... ima do the kid from tok[']s account send me \$700 off the play at least ima do [\$]4,800," by which L.S. meant that he planned to deposit a \$4,800 fraudulent check into D.P.'s Alaska USA account, and POST would transfer \$700 to L.S. from that deposit. POST agreed, replying "Okay I got you. And after we eat off that kids then [J.B.]?" L.S. replied "yeah," and POST followed up "her account is in good standing. Had it for like 3 years she said."

14. On September 3, 2020, POST deposited or caused to be deposited a fraudulent \$4,625 check drawn from MAC Federal Credit Union account ending in -3161 in victim J.H.'s name, into Alaska USA account ending in -3574 in "Play" B.S.'s name. POST utilized, without lawful authority, the name and bank account number of victim J.H. to commit this offense, knowing J.H. was an actual person.

15. On or about September 25, 2020, B.S. messaged POST over Instagram and asked “[w]ho deposited the money?” POST replied “I did. Out of that \$4,500 I want \$2,500. 705 Muldoon address. Don’t fuck around with peoples bread. I’m not threatening you in any way.”

16. On September 27, 2020, POST messaged Sun to “send my cut [\$2,500] through Walmart Moneygram or Fred Meyer Western Union.”

17. On or about December 18, 2020, POST and L.S. exchanged the following messages on Instagram regarding the conspiracy:

L.S.: I need money dude

POST: On [sic] god lol me too

L.S.: 😏😏

POST: I shouldn’t have fucked off all my bags smh

L.S.: No one left to scam lol

POST: O[h] god besides natives

POST: Homeless

L.S.: 😏😏😏

L.S.: Natives lol

...

POST: The only other choice is to get busy. I’m going car hoping tonight

I’m looking for checks and money lol

L.S.: 😏

L.S.: So serious lol

...

L.S.: Yeah hit the old looking cars honestly more likely to have change gift cards and money shit like that probley checks old people got the best fr

POST: O[h] god lol Im leaving at 1:30am

18. On or about October 26, 2020, unindicted co-conspirator L.P. and POST cashed or attempted to cash fraudulent checks at Mt. McKinley bank in Fairbanks, Alaska, for \$1,200 and \$750 drawn from Mt. McKinley Bank account ending in –3051 in the name of victim J.W.

//

//

//

//

//

//

//

//

//

//

//

//

//


//

CONCLUSION

19. Based on the aforementioned information, your affiant respectfully submits that there is probable cause to believe that JARED WILKES POST committed acts in violation of 18 U.S.C. § 1344(2) (bank fraud), violations of 18 U.S.C. § 1349 (conspiracy to commit bank fraud), and violations of 18 U.S.C. § 1028A (aggravated identity theft).

Your affiant requests the issuance of an arrest warrant for JARED WILKES POST.

Respectfully submitted,


Baron H. Lambert
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on June 6th, 2022:


HONORABLE SCOTT A. ORAVEC
UNITED STATES MAGISTRATE JUDGE

